DETAILED ACTION

1. Claims 20-36 are pending in the instant application and have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 34-36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The preamble of claims 34-36 indicate that they are directed towards a software product. However, the claims do not positively recite any limitation that specifies the software as being embodied in a *tangible* computer-readable medium, i.e., a non-transitory storage medium. The Applicant's Specification does not explicitly exclude the medium from comprising a non-statutory electromagnetic transmission medium and the claim scope must include this as well. Therefore the claim sets forth only functional descriptive language and is non-statutory since this does not fall into one of the classes of invention eligible for the grant of a US patent. Unless embodied in a computer-readable medium the software in and of itself cannot be considered as a computer component, and hence cannot effect a change of state of a processor to produce a useful or tangible result. From 2106.01: Computer-Related Nonstatutory Subject Matter: *Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when*

employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) *"Nonfunctional descriptive material" includes but is not limited to music, literary works, and a compilation or mere arrangement of data. Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. *When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases.*

The Applicant might consider amending these claims to explicitly set forth that the computer program element is embodied in a computer-readable storage medium.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 32, 33 and 36 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As for claims 32, 33 and 36, each of the claims recites a limitation wherein a server determines a refreshed decomposition. It is not apparent from the claim language what key is being acted upon, or how the server obtains the key.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 20-36 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Mittelholzer, International Application WO 00/49768 (submitted with Applicant's IDS).

Mittelholzer teaches:

As for claim 20, a method for cryptographically processing a message (abstract), wherein a first partial cryptographic key and a second partial cryptographic key, which correspond to a decomposition of a private cryptographic key, are used (page 3 lines 20-25, page 5 lines 7-20, page 5 line 27 through page 6 line 10); the message is processed using the first partial cryptographic key resulting in a first partially processed message (page 7 lines 4-23); the message is processed using the second partial

cryptographic key resulting in a second partially processed message (page 7 lines 4-23); the first partially processed message and the second partially processed message are combined resulting in a cryptographically processed message (page 7 lines 20-25), wherein further at selected times and after or before the message is processed a refreshed decomposition is determined and wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key (page 14 line 16 through page 15 line 25).

As for claim 21, the method according to claim 20, wherein the processing of the message using the first partial cryptographic key is carried out by a first computer and the processing of the message using the second partial cryptographic key is carried out by a second computer (page 6 lines 15-21).

As for claim 22, the method according to claim 21, wherein the first and the second computer are coupled via a computer network (page 6 lines 15-21, fig. 3).

As for claim 23, the method according to claim 21, wherein the method further comprises the step of transmitting the message from the first computer to the second computer (page 6 lines 15-28, fig 3).

As for claim 24, the method according to claim 20, wherein the first partial cryptographic key and the second partial cryptographic key correspond to a decomposition of the private cryptographic key into a plurality of partial cryptographic keys (page 14 line 16 through page 15 line 25).

As for claim 25, the method according to claim 24, wherein the plurality of partial cryptographic keys give, when summed, the private cryptographic key (page 14 line 16 through page 15 line 25).

As for claim 26, the method according to claim 20, wherein the cryptographical processing of the message is the signing of the message or the decrypting of a message (page 7 lines 4-23: signing).

As for claim 27, the method according to claim 20, wherein the message is processed according to a public key cryptographic algorithm (page 6 lines 15-30).

As for claim 28, the method according to claim 27, wherein the public key cryptographic algorithm is the RSA algorithm (page 9 lines 10-35: invention taught as useable with RSA).

As for claim 29, the claim is directed towards the apparatus which carries out the method of claim 1. Claim 29 recites substantially the same limitations as claim 1 and is thereby rejected on the same basis as that claim.

As for claim 30, a method for generating a cryptographically processed message (abstract) wherein a message is processed using a first partial cryptographic key, which corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message (page 3 lines 20-25, page 5 lines 4-23, page 5 line 27 through page 6 line 10), the message is transmitted to a client computer (page 6 lines 15-30, fig. 3); a second partially processed message is received which is the message processed using a second partial cryptographic key which corresponds to the decomposition of the private cryptographic key (page 3 lines 20-25, page 5 lines 4-23, page 5 line 27 through page 6 line 10); the first partially processed message and the second partially processed message are combined to a cryptographically processed message (page 7 lines 20-25), wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined, wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key (page 14 line 16 through page 15 line 25).

As for claim 31, the claim is directed towards the apparatus which carries out the method of claim 30. Claim 31 recites substantially the same limitations as claim 30 and is thereby rejected on the same basis as that claim.

As for claim 32, a method for performing a cryptographic operation on a message (abstract), wherein a message is received; the message is processed using a partial cryptographic key which corresponds to a decomposition of a private cryptographic key resulting in a partially processed message (page 3 lines 20-25, page 5 lines 7-20, page 5 line 27 through page 6 line 10, page 7 lines 4-23); the partially processed message is transmitted to a server computer, wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined (page 14 line 16 through page 15 line 25).

As for claim 33, the claim is directed towards the apparatus which carries out the method of claim 32. Claim 33 recites substantially the same limitations as claim 32 and is thereby rejected on the same basis as that claim.

As for claim 34, the claim is directed towards the computer program that directs a processor to undertake the method steps of claim 20. Claim 34 recites substantially the same limitations as does claim 20 and is thereby rejected on the same basis as that claim.

As for claim 35, the claim is directed towards the computer program that directs a processor to undertake the method steps of claim 30. Claim 35 recites substantially the same limitations as does claim 30 and is thereby rejected on the same basis as that claim.

As for claim 36, the claim is directed towards the computer program that directs a processor to undertake the method steps of claim 32. Claim 36 recites substantially the same limitations as does claim 32 and is thereby rejected on the same basis as that claim.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

/PEC/
AU2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437